UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/993,495	11/27/2001	Doug Rollins	M4065.0486/P486	8165

24998 7590 10/12/2010

DICKSTEIN SHAPIRO LLP
1825 EYE STREET NW
Washington, DC 20006-5403

EXAMINER	
GELAGAY, SHEWAYE	

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
10/12/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/993,495
Filing Date: November 27, 2001
Appellant(s): ROLLINS, DOUG

Gianni Minutoli
Reg. No. (41,198)
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 07/22/10 appealing from the Office action mailed 09/11/09.

(1) Real Party in Interest

The examiner has no comment on the statement, or lack of statement, identifying by name the real party in interest in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The following is a list of claims that are rejected and pending in the application:

Claims 1-12 and 14.26.

(4) Status of Amendments After Final

The examiner has no comment on the appellant's statement of the status of amendments after final rejection contained in the brief.

(5) Summary of Claimed Subject Matter

The examiner has no comment on the summary of claimed subject matter contained in the brief.

(6) Grounds of Rejection to be Reviewed on Appeal

The examiner has no comment on the appellant's statement of the grounds of rejection to be reviewed on appeal. Every ground of rejection set forth in the Office action from which the appeal is taken (as modified by any advisory actions) is being maintained by the examiner except for the grounds of rejection (if any) listed under the

subheading "WITHDRAWN REJECTIONS." New grounds of rejection (if any) are provided under the subheading "NEW GROUNDS OF REJECTION."

(7) Claims Appendix

The examiner has no comment on the copy of the appealed claims contained in the Appendix to the appellant's brief.

(8) Evidence Relied Upon

7,024,553	Morimoto	04-2006
6,055,314	Spies et al.	04-2000
4,369,332	Campbell, Jr.	01-1983
6,226,570	Trieger	05-2001

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1, 6-8, 14-20 and 26 rejected under 35 U.S.C. 103(a) as being unpatentable over Morimoto US 7,024,553 in view of Spies et al. (hereinafter Spies) US 6,055,314.

As per claim 1:

Morimoto teaches a method of updating and using an encryption key used by a wireless station for encrypted communications with a wired portion of the network, said method comprising:

connecting to a key updating device which is connected to a wired portion of said network said wired portion of said network containing an encryption key generator for providing a new encryption key to said updating device; (col. 7, lines 51-67; col. 8, lines 25-61)

connecting a network communications device to an encryption key updating device which is connected to a wired portion of said network said wired portion of said network containing an encryption key generator for providing a new encryption key to said updating device; (col. 7, lines 51-67; col. 8, lines 25-61)

replacing an existing encryption key in said network communications device with a new encryption key from said generator sent over said wired portion of said network; (col. 7, lines 51-67; col. 8, lines 25-61)

reconnecting said network communications device containing said new encryption key with said wireless station of said network. (col. 7, lines 51-67; col. 8, lines 25-61) and

accessing said new encryption key during an encrypted communication. (col. 7, lines 51-67; col. 8, lines 25-61)

Morimoto does not explicitly physically separating a wireless network device and physically reconnecting the wireless communication device from a wireless station.

Spies in analogous art, however, discloses physically separating a wireless network device and physically reconnecting the wireless communication device from a wireless station. (col. 6, lines 10-32) Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Morimoto with Spies in order to implement decryption capabilities on the IC card without exposing the decryption capabilities, thereby providing secure delivery system that permits easy replacement of security protocol. (Abstract; col. 2, lines 16-18; Spies)

As per claims 6-7, 14, 16 and 26:

The combination of Morimoto and Spies teaches all the subject matter as discussed above. In addition, Spies further discloses a method wherein said network communications device is configured on a plug-in card and is physically connection to said network by inserting said network communications device into a card tray at said updating device. (col. 6, lines 10-32)

As per claims 8 and 15:

Morimoto teaches a network comprising:

a wired station connected to a wired network, (col. 7, lines 51-67; col. 8, lines 25-61) said wired station comprising:

an encryption key generator for generating an encryption key; (col. 7, lines 51-67; col. 8, lines 25-61)

a network communication device for transmitting said encryption key over said wired network; (col. 7, lines 51-67; col. 8, lines 25-61) and

a wired encryption key updating device connected to said wired network; (col. 7, lines 51-67; col. 8, lines 25-61)

a wireless station configured to be wirelessly connected to said network and to communicate with said wired network through communications encrypted with an encryption key, (col. 7, lines 51-67; col. 8, lines 25-61) said wireless station comprising:

a wireless network communication device containing an encryption key, being disconnectable from said wireless station and connectable said wired encryption key updating device wired to said network to receive, store and use a new encryption key which is configured to be transmitted over said wired network by said wired network communications device. (col. 7, lines 51-67; col. 8, lines 25-61)

Morimoto does not explicitly disclose a wireless network device being physically disconnectable from the wireless station and physically connectable to said wired encryption updating device. Spies in analogous art, however, discloses a wireless network device being physically disconnectable from the wireless station and physically connectable to said wired encryption updating device. (col. 6, lines 10-32) Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Morimoto with Spies in order to implement decryption capabilities on the IC card without exposing the decryption capabilities, thereby providing secure delivery system that permits easy replacement of security protocol. (Abstract; col. 2, lines 16-18; Spies)

As per claim 17:

Morimoto teaches a wireless network communications device comprising:

A removable wireless communications network card adapted to be connected to and disconnected from a wireless station card interface; (col. 7, lines 51-67; col. 8, lines 25-61)

a storage area said network card which stores an updateable encryption key for use in conducting encrypted wireless network communications, (col. 7, lines 51-67; col. 8, lines 25-61) said encryption key being updateable when said card is connected to a wired network card interface which supplies a new encryption key. (col. 7, lines 51-67; col. 8, lines 25-61)

Morimoto does not explicitly disclose a wireless network device being physically connected to a wired network card interface which supplies a new encryption key. Spies in analogous art, however, discloses a wireless network device being physically connected to a wired network card interface which supplies a new encryption key. (col. 6, lines 10-32) Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Morimoto with Spies in order to implement decryption capabilities on the IC card without exposing the decryption capabilities, thereby providing secure delivery system that permits easy replacement of security protocol. (Abstract; col. 2, lines 16-18; Spies)

As per claims 18 and 19:

The combination of Morimoto and Spies teaches all the subject matter as discussed above. In addition, Spies further discloses a method wherein card interface for providing a new encryption key is a PCMCIA card interface. (col. 6, lines 10-32)

As per claim 20:

Morimoto teaches an encryption key programming system comprising:

an encryption key generator connected to a wired network; (col. 7, lines 51-67; col. 8, lines 25-61)

a programming device connected to said wired network for receiving over a wire connection an encryption key from said generator, said programming device being adapted to receive a wireless network communications device containing an updatable encryption key and storing said received encryption key in said wireless network communications device. (col. 7, lines 51-67; col. 8, lines 25-61)

Morimoto does not explicitly disclose a programming device adapted to physically receive a wireless network communications device Spies in analogous art, however, discloses a wireless network device being physically connected to a wired network card interface which supplies a new encryption key. (col. 6, lines 10-32) Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Morimoto with Spies in order to implement decryption capabilities on the IC card without exposing the decryption capabilities, thereby providing secure delivery system that permits easy replacement of security protocol. (Abstract; col. 2, lines 16-18; Spies)

3. Claims 2-3, 9-10 and 21-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Morimoto US 7,024,553 in view of Spies et al. (hereinafter Spies) US 6,055,314 and in view of Campbell, Jr. U.S. Patent 4,369,332.

As per claims 2-3, 9-10 and 21-23:

The combination of Morimoto and Spies teaches all the subject matter as discussed above. Both references do not explicitly disclose a method wherein said new encryption key is generated at user-defined intervals or on user-specified days. Campbell in analogous art, however, discloses a method wherein said new encryption key is generated at user-defined intervals or on user-specified days. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Morimoto and Spies with Campbell Spies in order to implement decryption capabilities on the IC card without exposing the decryption capabilities. (Abstract; Spies)

4. Claims 4-5, 11-12, 24-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Morimoto US 7,024,553 in view of Spies et al. (hereinafter Spies) US 6,055,314 and in view of Trieger United States Letter Patent Number 6,226,750.

As per claims 4, 11 and 24:

The combination of Morimoto and Spies teaches all the subject matter as discussed above. Both references do not explicitly disclose a method wherein said key generator generates a first new encryption key; compares said new encryption key to the previous k encryption keys used in said network; and generates a second new encryption key if said first new encryption key matches any of said k previously used encryption keys.

Trieger in analogous art, however, discloses a method wherein said key generator generates a first new encryption key; (Col. 11, lines 30-32) compares said new encryption key to the previous k encryption keys used in said network; (Col. 11,

lines 39-41) and generates a second new encryption key if said first new encryption key matches any of said k previously used encryption keys. (Col. 11, lines 38-43)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Morimoto and Spies with Trieger to include wherein said key generator generates a first new encryption key; compares said new encryption key to the previous k encryption keys used in said network; and generates a second new encryption key if said first new encryption key matches any of said k previously used encryption keys. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Trieger (Col. 11, lines 38-39) in order to ensure the previous key is not reused.

As per claims 5, 12 and 25:

The combination of Morimoto, Spies and Trieger teaches all the subject matter as discussed above. In addition, Trieger further discloses a method wherein k is a user-defined number of previously used encryption keys. (Col. 11, lines 38-43)

(10) Response to Argument

With respect to Appellant's argument section A.1:

Appellant argued that "*Morimoto explicitly teaches away from physical attachment of a separated network communication device to a wired encryption key updating device; further, combination with Spies would frustrate Morimoto's purpose.*" Appellant further argued that "*Although the present application and Morimoto are both*

directed to updating encryption keys on a corporate network, their methods are quite different. Morimoto explicitly teaches that "each STAs 103 memorizes and supervises …[new] encrypted key[s] delivered from the key management server 101 [wirelessly]." By contrast, the present application teaches updating the encryption key in use on the access point itself, but also updating an encryption key on an updating device (e.g., a PC card tray 400), so that wireless communications devices can be physically connected to that device for updating." This is especially important because the present application contemplates and distinguishes itself from a Morimoto-type wireless updating system, ... Morimoto delivers keys to wireless stations directly, and only, through its access points."

Examiner would like to point out that as admitted by Appellant's argument above both Morimoto and the current application are directed to updating encryption key in a wireless system from a corporate network. In order to clearly understand the claimed limitation the Examiner would like to point out that "**a wired portion of the network**" is merely **a conventional personal computer with PCMCIA card tray.** The specification recites *"When an encryption key is to be updated, the wireless network communications device card is removed from the wireless station and inserted into a card tray connected to a wired portion of the network. A management station randomly generates a new key and propagates it to all access points and to one or more card trays. The card trays may be conventional personal computer card trays, e.g. PCMCIA or other PC card trays. Once encryption key is updated and the encryption key in each of the wireless network communication devices is updated. The wireless network communications devices*

having updated encryption keys may then be removed from the card trays and reinserted into the wireless stations." (see [0013]) And further recites "*The card try may receive any type of conventional computer card ...but for the purpose of simplifying discussion, it will be assumed the network communication devices are provided on a PCMCIA card that card tray receives such cards.*" (see [0020])

Morimoto teaches updating encrypted key to a wireless LAN system having plural Access Points (APs) and a large number of STAs. ***A key management server is LAN connected to the APs*** and the key management server generates and supervises an encrypted key or keys used for encryption. On generation of a new key, the key management server delivers it to the AP and STAs. When the encrypted key is delivered to the AP, the latter updates an encrypted key used for communication with the STAs to memorize and supervise the updated encrypted key as well as to advise STAs for the updating of encrypted key. (i.e. *updating encrypting keys from a wired network to a wireless device*) Then each of STAs memorizes and supervises the encrypted key delivered from the key management server through the AP and has communication with the AP using the encrypted key. (see Figure 1; col. 7, 50-col. 8, line 4) Morimoto teaches a system and method of updating encryption key for wireless LAN having a plural APs and a large number of STAs. A key management server is LAN-connected to the APs. (Abstract) The STA on reception of a notification on key updating from the AP requests the key management server to update the key through the AP. If the key server verifies that the delivery of the STA key is possible, the encrypted key is delivered to the STA through the AP. (col. 9, lines 45-53) The encrypted key updating is

performed at a rate of one encrypted key, e.g., per week. By so doing, the respective encrypted keys are updated once every four weeks. Therefore, a person carrying a portable STA outwards can access to the AP (APs) unobjectionably if the STA is returned within four weeks. (col. 12, line 18-23) Morimoto teaches updating encrypted keys to wireless stations from a LAN connected APs and supervising, memorizing the updated keys to effect encrypted communication on a wireless station. Therefore, Morimoto teaches all the limitation recited in claim 1 except *"physically separating a network communication device and physically connecting said separated network communication device to key updating device and physically reconnecting said network communication device."*

Spies teaches an IC card , such as smart card or PCMCIA card, that stores keys and configured with cryptographic functionality to support the secure purchase and delivery of content. The IC card operates in conjunction with a viewer's computing device to decrypt the content without exposing the decryption capabilities and decryption keys. The purchaser physically carries the IC card, such as PCMCIA card with processing chip, and presents it to the video merchant. The video merchant inserts the IC card into a compatible I/O device connected to the merchant's computing unit at the merchant's premises. If the IC card is verified, the merchant computing unit transfers the cryptographic program key for the selected program from the secure key store to the IC card. At home the purchaser inserts the IC card into the disk player or other computing unit to decrypt the program. (col. 6, lines 11-32) Therefore, Spies teaches an IC card that can be separated from the computing unit (i.e. physically

separating network communication device) and taken to the merchant's computing unit at the merchant's premises to update a cryptographic key (i.e. physically connecting said separated network communication device to a wired network) and inserting the IC card at the computing unit to decrypt a program (i.e. physically reconnecting said network communication device) which is adequate to meet the claimed limitation.

Because both Morimoto and Spies teach a method of transferring and protecting cryptographic keys, it would have been obvious to one skilled in the art to substitute one method for the other to achieve the predictable result of transferring keys without exposing the keys to unauthorized access. (*KSR International Co. v. Teleflex, Inc.*, 550 U.S. 398, 82 USPQ2d 1385 (2007)) As discussed above, the references do not teach away from the combination because both Morimoto and Spies teach securely delivering cryptographic keys Morimoto uses delivering keys wirelessly from the wired portion and Spies teaches physically taking an IC card to a computing device and updating the keys. Therefore, the references do not teach away from the combination and it would have been obvious to one ordinary skill in the art to combine Morimoto and Spies.

With respect to Appellant's Argument Section A.2.

Appellant argued that "*Even if Morimoto and Spies could be combined, Spies cannot cure the deficiencies of Morimoto ... Spies merely teaches distributing decryption keys on a removable IC cards (e.g, PCMCIA cards) to enable a video player to decode video content stored on a DVD or other medium. Spies' IC cards are not network communication devices, nor do they provide "encryption key[s] used by a wireless station for encrypted communication devices with a wired portion of the network. ..In*

fact, separable network communications devices are not taught or suggested anywhere in either Morimoto or Spies."

First, the Examiner would like to point out that a "*network communication device*" has not been explicitly defined by the specification. The specification recites "*Wireless network communication device can be a wireless network interface card.*" (see [0006]) and the key updating device is described as "*The card trays may be conventional personal computer card trays ,e.g. PCMCIA or other PC card trays.*" (see [0013]) Second, Spies teaches the purchaser has an IC which can be compatibly interfaced to the merchant computing unit, either through direct connection or via a remote link. The IC card is a portable card-like device that has processing capabilities. The purchaser physically carries and presents the IC card to the merchant and if the card is verified, the merchant computing unit transfers the key to the card. At home, the purchaser inserts the IC card into the computing unit that in the form of an STB, a desktop or a portable computer to decrypt the content. Therefore, Spies teaches physically separating IC card from the purchaser computing unit (i.e. portable computer) and physically connecting the card to the merchant computing unit and reconnecting the card to a wireless network communication device.

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). In this case, Morimoto discloses a method for updating encryption key for

wireless LAN from an AP that is LAN connected to a key server and updating the keys wirelessly from the AP to the wireless station. Spies teaches using an IC card to transfer a key from a merchant station to avoid exposing the keys. One ordinary skill in the art at the time the invention was made would have found it obvious to update the keys between the wired portion of the network and the wireless station using an IC card and thereby gain, predictably, a secure and reliable key delivery.

With respect to Appellant Argument Section B.

Appellant's argument with this section has been addressed in Section A.1 and A.2 above.

With respect to Appellant Argument Section C.

Appellant's argument with this section has been addressed in Section A.1 and A.2 above.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Shewaye Gelagay/

Examiner, Art Unit 2437

Conferees:

Matthew Smithers
/Matthew B Smithers/

Primary Examiner, Art Unit 2437

Emmanuel Moise
/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437